PROCEDURE

Mise en Place du FSRM

Et de la tâche planifiée NOCRYPTO

** ALTAE GROUPE**

**137, Rue Mayoussard  
PARC POMMARIN  
38430 MOIRANS**

**04 76 35 49 94**

Ces scripts ont pour but d’utiliser une liste d’extensions connues comme utilisées par les ransomwares et de les intégrer au gestionnaire de ressource de fichiers (Rôle FSRM) afin d’interdire leur utilisation sur le serveur. Si un crypto est exécuté sur un poste, le cryptage des fichiers sur le serveur ne sera pas possible.

Dans cette procédure, nous allons voir comment installer le rôle FSRM, déployer le script, le mettre en tâche planifiée et enfin gérer les exclusions manuellement (exclusions de partage et exclusions d’extension.

# 1 : PRE-REQUIS :

Cette procédure n’est pas applicable à des serveurs Windows Server 2003.

Elle s’applique aux serveur 2008, 2008R2, 2012, 2012 R2 et 2016.

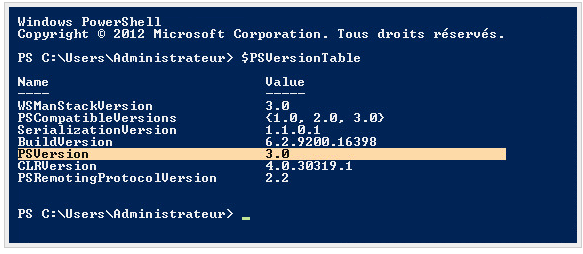
Pour le moment le script ne peut pas fonctionner sur les serveurs Exchange

### Vérifier la présence de Powershel V3 minimum

Il est primordial de vérifier sur le serveur la version de Powershell car le script ne fonctionnera pas pour les version antérieur à V3.

Pour vérifier la version de Powershell, il suffit de lancer en ligne de commande :

**$PSVersionTable**



Pour passer un serveur 2008R2 en Powershell 3 il faudra installer successivement

* .Net Framework 4 : <http://www.microsoft.com/fr-fr/download/details.aspx?id=17718>
* Windows Management Framework 3.0 : <http://www.microsoft.com/en-us/download/details.aspx?id=34595>

### Installation du rôle FSRM

Pour mettre en place cette tâche planifiée, il nécessaire auparavant d’installer le rôle du Gestionnaire de ressources du serveur de fichier. Il y a pour cela deux possibilités :

1. Via un script Powershell : veiller à exécuter le bon script selon si l’on utilise un Windows Server 2008 ou 2012

Pour 2008

**Import-Module Servermanager**

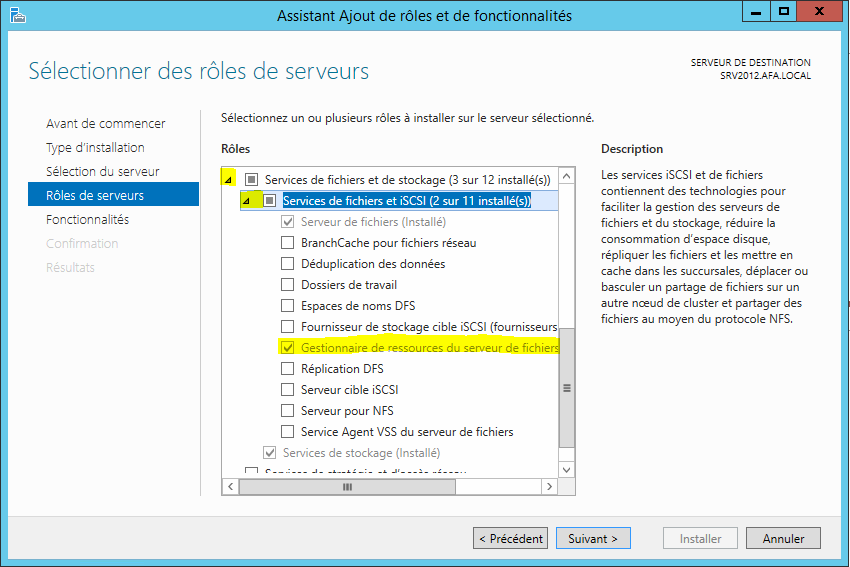
**Add-WindowsFeature FS-Resource-Manager**

Pour 2012

**Import-Module ServerManager**

**Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools**

1. Manuellement, en ajoutant un rôle (**méthode à préférer**) :



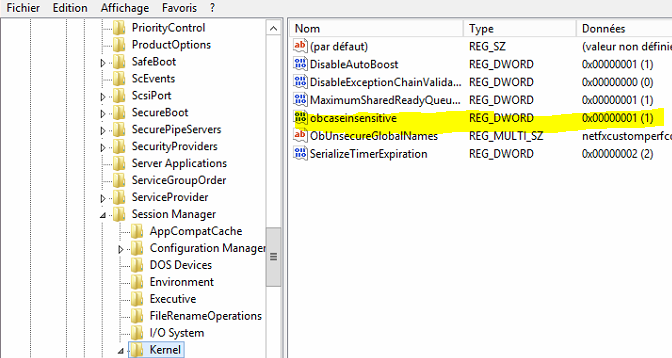
Faire la vérification de la base de registre suivante avant de redémarrer le serveur

### Modification de la base de registre

Sur certains serveur, il est nécessaire de modifier la base de registre pour forcer Windows à être sensible à la casse. Cette action est nécessaire car les crypto évoluent souvent et c’est bête de se retrouver crypté par une extension en \*.Crypt alors que l’on avait interdit l’extension \*.crypt

Pour se faire, il suffit de vérifier que la clé

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel obcaseinsensitive** est à 1

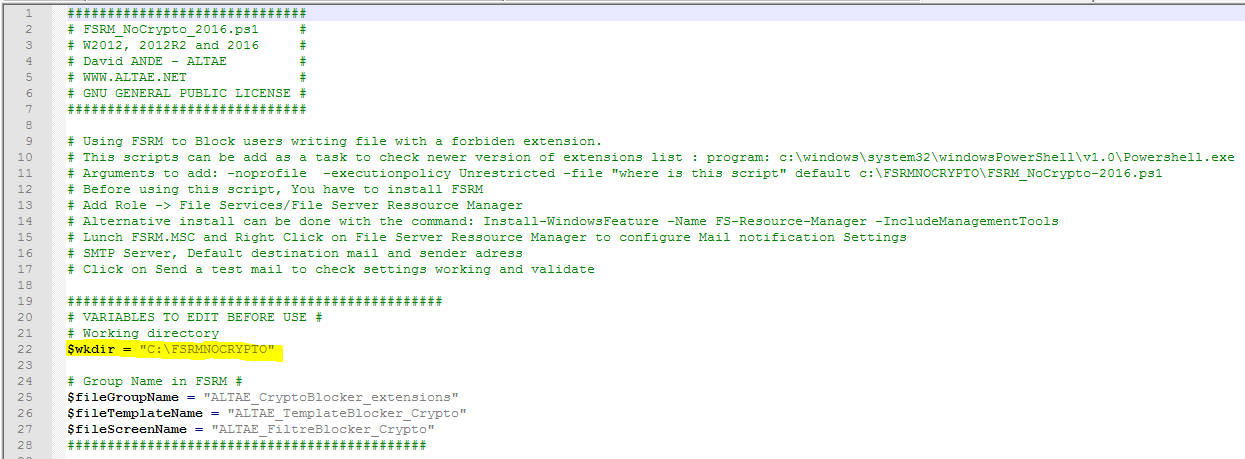


# 2 : INSTALLATION :

Téléchargez l’intégralité de l’archive sur : <https://github.com/davidande/FSRM-ANTICRYPTO> en cliquant sur Clone or Download et en choisissant Download ZIP

Sur le serveur vous devrez créer un dossier **C:\FSRMNOCRYPTO** dans lequel il faudra dézipper l’archive. (attention, pas de sous répertoire, tous les fichiers doivent se retrouver à la racine du dossier **C:\FSRMNOCRYPTO.**

Si vous souhaitez pour une raison changer le répertoire des scripts (ce que je ne conseille pas), il faudra modifier la variable **$wkdir** du script.



**TEST DU SCRIPT**

Il y a deux scripts :

L’un est pour être utilisé sur les serveur 2008 et 2088 R2 **FSRM\_NoCrypto\_2008.ps1**

L’autre sur les serveurs 2012, 2012R2 et 2016 **FSRM\_NoCrypto\_2016.ps1**

Pour une plus grande lisibilité, je vous conseille de lancer **POWERSHELL ISE** , d’y ouvrir le script et de le lancer. Cette méthode permet de lire les erreurs s’il y en a.

Au premier lancement, il devrait y avoir des erreurs, c’est normal.

Pour vérifier à nouveau que le script fonctionne, il faut au préalable modifier le fichier extensions.old se trouvant dans le répertoire des scripts. Ouvrez ce fichier avec Notepad, modifier quelques caractères et enregistrez-le.

Ce fichier extensions.old est utilisé par le script pour comparer la liste des extensions utilisées en local avec la liste d’extension disponible à distance.

S’il n’y a pas de différence entre les deux listes, le script s’arrete car pas de nouvelles extensions trouvées. Donc pour forcer l’exécution complète du script, il suffit de modifier simplement le fichier extensions.old. ATTENTION le fichier extensions.old ne doit jamais être vide.

La deuxième exécution doit se passer sans erreur. S’il y en a, ce n’est pas normal (donc appeler David Andé)

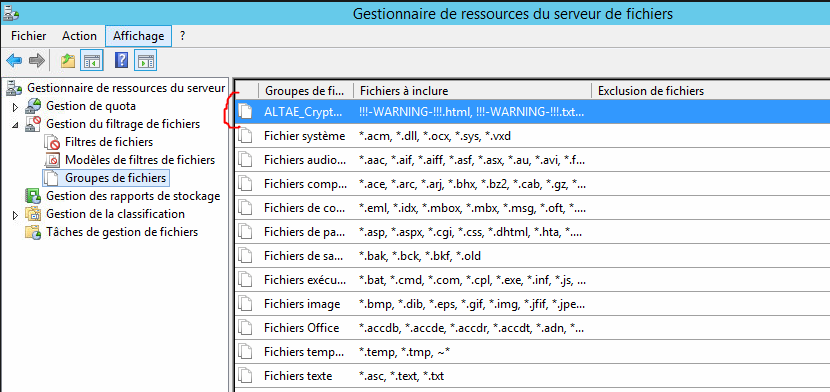
**Vérification dans la console du gestionnaire de ressources du serveur de fichiers**

**(accessible aussi en ligne de commande fsrm.msc)**

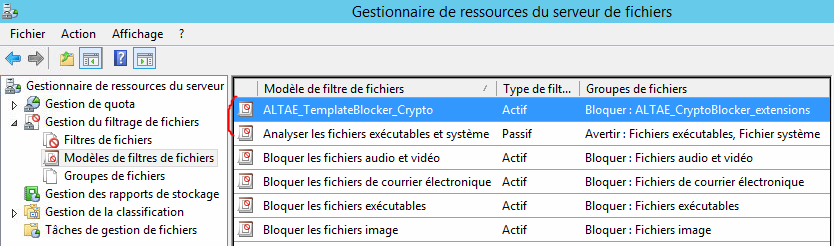
Le gestionnaire de ressources du serveur de fichier a été renseigné dans la partie *Gestion du filtrage de fichier* :

1. Dans un premier temps, le script créé un groupe de fichiers nommé *ALTAE\_CryptoBlocker\_extensions* dans lequel sont listés tous les noms de fichiers et extensions qui ont été mis à jour dans le fichier *extensions.old* :

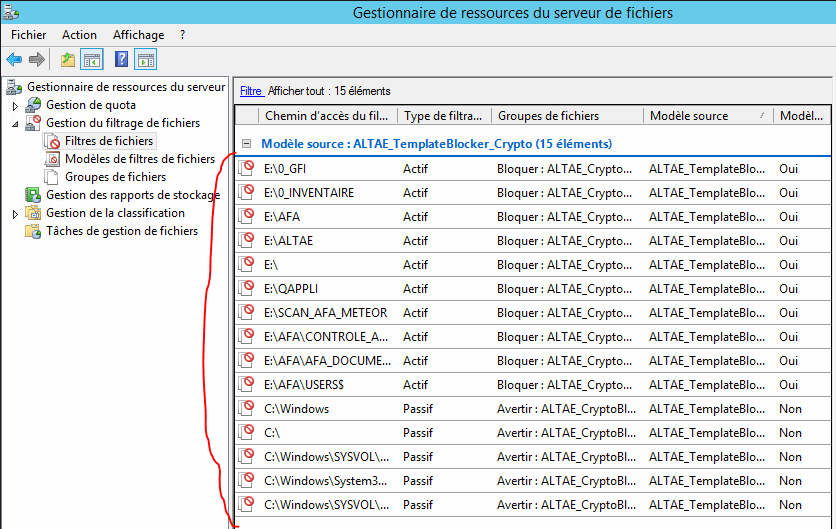
Pour les version < à 2012, Il y aura plusieurs listes car leur taille étant limité à 4kb, une seule ne permet pas d’accueillir la très grande liste des extensions à exclure).



1. Ensuite, est créé un modèle de filtres nommé *ALTAE\_TemplateBlocker\_Crypto* qui définit les paramètres du filtrage, ici : qu’il est actif et qu’il bloque la création de fichiers ou extensions définis dans le groupe ci-dessus :



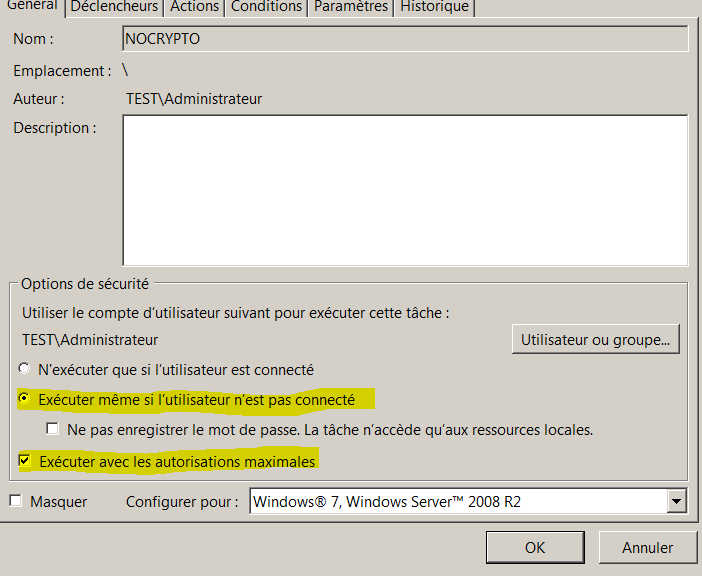
1. Le modèle est enfin appliqué aux différentes partitions et partages du serveur. A noter que pour la partition C:\, le filtrage n’est jamais *Actif*  pour les partage administratifs. Par contre s’il y a des partages autres qu’administratifs sur le C, le filtrage se fera en *Actif* et non en passif.



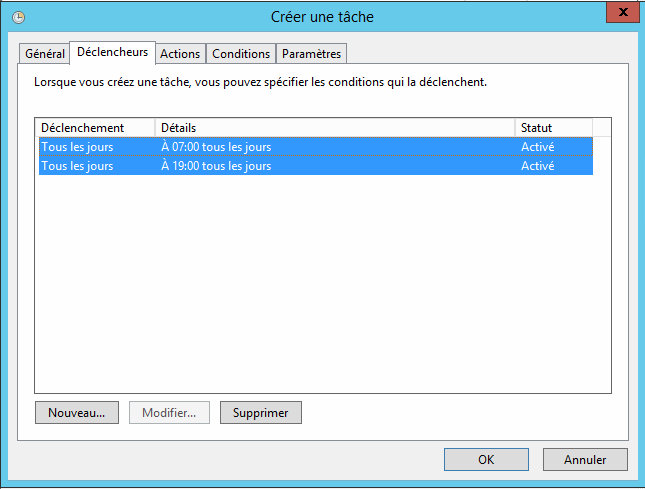
**ACTIF ou PASSIF : par défaut l’application de la protection est en ACTIF, c’est-à-dire application complète de l’interdiction. Pour les partages liés au système, le filtrage est en PASSIF (c’est Windows qui gère çà, impossible de forcer). La protection passive n’interdit pas l’ecriture d’une extension interdite, mais renseigne tout de même le journal d’événements.**

## Mise en place de la tâche planifiée

Une fois le bon fonctionnement validé, il faut mettre en place la tâche planifiée qui viendra mettre à jour automatiquement la liste des fichiers et extensions à bloquer, puis mettre à jour également le gestionnaire du filtrage des fichiers :



Le déclenchement est à définir selon les besoins, 2 fois par jour en dehors des horaires des utilisateurs parait correcte mais vous pouvez tout à fait l’exécuter toutes les heures car sont lancement ne génère aucune lenteur.

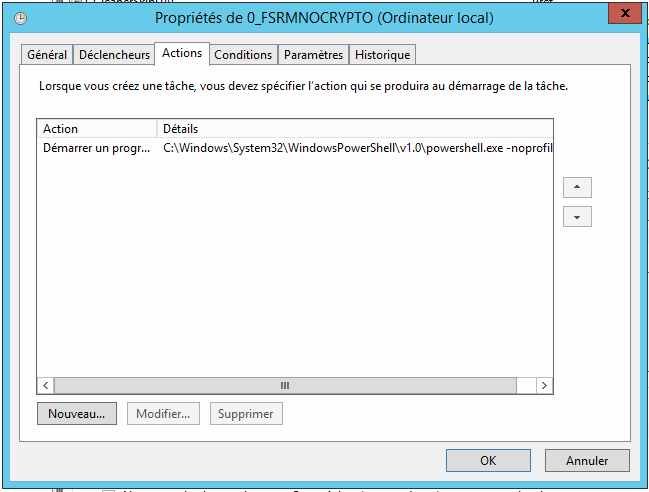


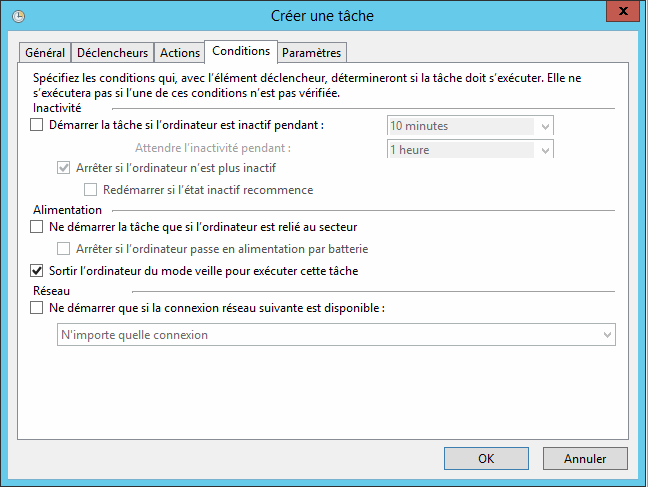
L’action à définir, n’est pas directement l’exécution du script, mais l’exécution de Powershell avec des arguments.

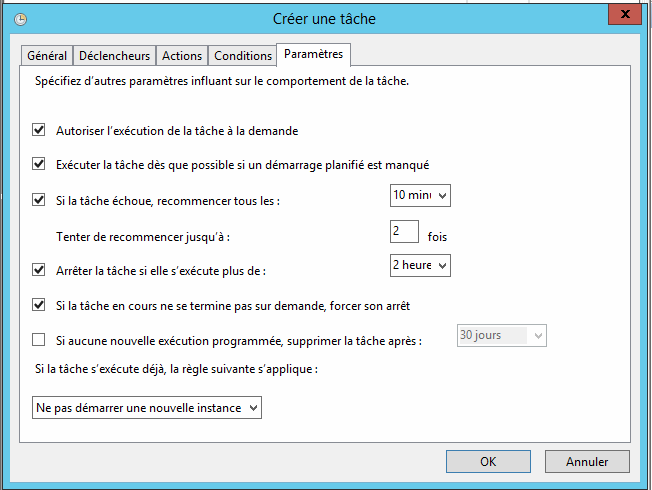
Le programme a exécuter est donc : ***C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe***

Avec les arguments : ***-noprofile -executionpolicy Unrestricted -file "C:\FSRMNOCRYPTO\FSRM\_NoCrypto\_2016.ps1" (ou version 2008)***

Avec le paramètre *-file* à définir selon la localisation du script sur le serveur.







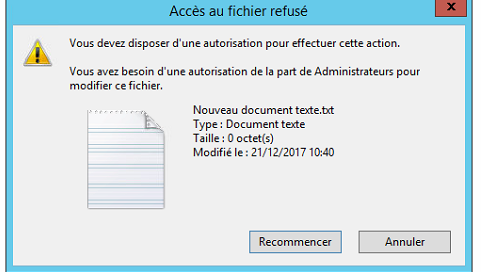
La tâche planifiée est donc paramétrée, bien penser à vérifier de temps en temps le bon fonctionnement de la mise à jour du fichier *extensions.old* et aussi du gestionnaire du filtre des fichiers.

## Tester le bon fonctionnement du service

Pour vérifier que tout fonctionne, il suffit de provoquer la protection en écrivant un fichier avec une extension interdite.

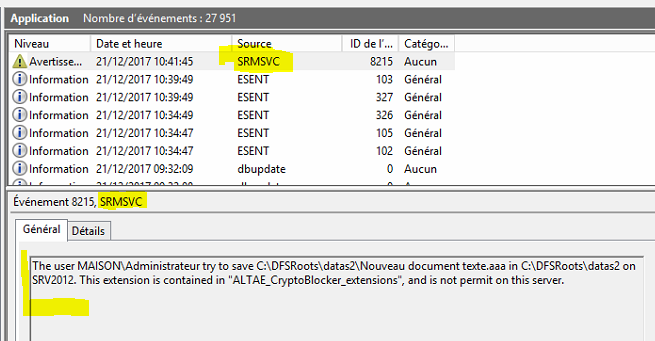
Allez dans un partage, créez un nouveau fichier et changez son extension en .aaa

Vous devriez obtenir le message d’alerte suivant



Donc ca marche.

On trouve aussi un événement dans le journal d’événement Application



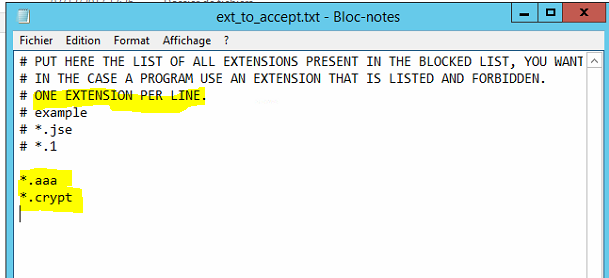
## Gestion des exclusions (Bypass)

Il est possible de gérer des exclusions, c’est-à-dire d’une part d’autoriser des extensions interdites ou exclure des partages de la protection FSRM

### Autorisation d’extensions interdites

Il est possible d’autoriser une exclusion interdite. Cette autorisation se fait en renseignant le fichier ext\_to\_accept.txt

Dans mon exemple, je vais autoriser l’extension aaa et crypt (c’est pas bien !!!!)



Il faut alors relancer le script (avec au préalable la modification du fichier extensions.old si vous avez bien suivi 😊)

Et tester l’écriture d’un fichier avec ces extensions.

### Autoriser un partage à bypasser la protection.

C’est nécessaire lorsqu’il y a des clés USB dongle ou d’autres média dont la protection ne peut pas s’appliquer ou pose problème

Cette partie se gère directement dans le script. C’est cette section

# Drives to exclude for FSRM bloking

# If You want to exclude complete Path or special directory so write for exemple "C:\share" for specific share

# or "D:\shar\*" for all shares in D starting by shar or "E:\\*" for all shares in E

# or"D:\\*shar\*"for all shares in D containing shar.

# If nothing to exclude let the value to "0". only one value per line so only 2 exclusions for the moment :-)

# ex: $drive\_exclu1= "C:\Windows\*"

$drive\_exclu1 = "0"

$drive\_exclu2 = "0"

Une fois le script modifié, il faudra aller dans la console FSRM et supprimer le partage à exclure.

Si vous relancez le script (après modif d’extensions.old), le partage ne devrait plus apparaitre dans la console FSRM

**Attention à bien rafraichir la console car son affichage n’est pas dynamique**

# 3 : FAQ / DIVERS / A NOTER etc… :

Sources : <https://github.com/davidande/FSRM-ANTICRYPTO>